2008

The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation

Gaurav Bansal
University of Wisconsin - Green Bay, bansaig@uwgb.edu

Fatemeh "Miriam" Zahedi
University of Wisconsin - Milwaukee, zahedi@uwm.edu

David Gefen
Drexel University, gefend@drexel.edu

The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation

Completed Research Paper

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

Fatemeh "Mariam" Zahedi
University of Wisconsin – Milwaukee
zahedi@uwm.edu

David Gefen
Drexel University
gefend@drexel.edu

ABSTRACT

Privacy policy statements and privacy-assurance cues are among the most important website features that online providers use to alleviate web customers' privacy concern. This study examines the moderating role of privacy concern on how the quality of privacy policy statements and privacy assurance cues contribute to increased trust, and the subsequent decision to disclose private information online. The results of this study show distinct behavioral differences between how individuals with high versus low privacy concern form their trust to disclose private information across different contexts. The paper adds to the trust literature by highlighting the influence of the customer's level of privacy concern (as who) and of the context (as where). The paper also adds to the Elaboration Likelihood Model Theory (ELM) by demonstrating the combined moderating roles of context and degree of involvement (privacy concern).

Keywords: Information privacy, Trust, Elaboration likelihood theory, Privacy assurance cues, Privacy policy statement quality, privacy concern

TITLE AND ABSTRACT IN FRENCH

L'effet modérateur du souci de confidentialité sur l'efficacité des mécanismes de respect de la vie privée à construire la confiance : une investigation en contextes multiples

Résumé:
Cette étude examine le rôle modérateur de la préoccupation de confidentialité sur la manière dont la qualité des déclarations de confidentialité et les signaux d'assurance de confidentialité renforcent la confiance, et en conséquence la décision de divulguer des renseignements personnels en ligne. Les résultats de cette étude montrent des différences de comportement entre la manière dont les individus forment leur confiance pour divulguer des renseignements personnels dans des contextes différents, selon qu'ils sont très soucieux à propos de la confidentialité ou qu'ils sont moins.

Introduction

Research (e.g., McKnight et al. 2002; Malhotra 2004) shows that a trusted online environment results in customers' increased tendency to disclose their private information online. Privacy-policy statements and privacy-assurance cues are among the most important website features that online providers can use to create a trusted online environment that could alleviate their web customers' privacy concerns (Milne and Culnan 2002, 2004). Currently, the examination of the role of online privacy policies in creating a trusted environment has been either limited to their mere presence (as a "trust cue"), or has been ignored in the literature (Milne and Culnan 2004). Metzger (2006) notes with surprise that no studies have investigated the effects of privacy policy content variations on consumer attitudes and behavior. The converse is also true. There is little knowledge about the effects of personal attitudes on the way privacy policies are perceived (Hui et al. 2007). To address this gap, this paper poses the following research question: Does customers' privacy concern moderate the effect of the perceived quality of the privacy-policy statement and its peripheral cues on trust when disclosing private information online?

The study formulates a conceptual model based on the elaboration likelihood model (ELM) as the overarching theory. ELM (Petty and Cacioppo 1986) states that people in the high elaboration likelihood state (high privacy concern, in this case) are more likely to engage in thoughtful processing of an information message (privacy-policy statement), and, therefore, are more persuaded by argument quality (the quality of the privacy-policy statement). This is called the central route. In contrast, those in the low elaboration likelihood state (low privacy concern, in this case), lacking the motivation to scrutinize the message (privacy-policy statement), tend to rely more on peripheral cues (privacy assurance cues) in making a judgment about the message. This is called the peripheral route.

In this study, we develop scales to measure the perceived quality of a privacy-policy statement in terms of its understandability and adequacy. Adequacy is a second-order construct that comprises of four dimensions—collection, errors, secondary use, and improper access. Peripheral cues are formulated and measured in terms of information quality, website design quality, third party assurances, and perceived presence of company information. Trust and the intention to disclose private information online are the dependent constructs.

To establish the generalizability of the results and to examine the influence of external "context" (Bansal et al. 2008, Johns 2006), we examine the model across three different domains: finance, e-commerce, and health. The research methodology is a controlled lab experiment with random assignment of context stimuli. The data analysis method is structural equations modeling. Comparisons are carried out using chi square and t-tests. This study has both theoretical and managerial contributions. To our knowledge, this study is the first to highlight the differential impact of privacy assurance mechanisms as moderated by high versus low privacy concerns when disclosing private information online in three different contexts. The findings provide guidelines for managers on a variety of ways to build trust in contexts where users are asked to provide private information online.

Literature Review

Milne and Culnan (2002) reported on the evolution of online privacy-policy statements posted by US companies and argued that both the content (related to fair usage of information—adequacy of privacy-policy statement) and format (understandability) of the privacy-policy statement are important in creating a trusting environment. However, these privacy-policy statements vary in terms of their place on the website, their length, ease of reading, and the level of guaranteed protection (Liu et al. 2002). Furthermore, since people have different levels of privacy concern, we argue that not all people are *equally* influenced by the "quality" of such statements. Milne and Culnan (2002) observed that experience with the company, its reputation, and the presence of privacy seals could serve as alternatives to a privacy-policy statement. This assertion is supported by Benassi (1999), who argued that displaying seals of approval may add trustworthiness and credibility to corporate websites by suggesting that the company is willing to have its privacy practices audited. However, recent studies note that privacy seals are no guarantee against infringement of users' privacy (e.g., Pollach 2006).

Overarching Theory: Elaboration Likelihood Model (ELM)

Cognitive energy spent on processing a message may vary among individuals in different contexts (Petty and Cacioppo 1986). The variations in cognitive elaboration, *ceteris paribus*, may affect the extent of a message's

influence. According to Petty and Cacioppo (1986), elaborating on a message requires ability and motivation. ELM suggests that when elaboration is high, the recipient experiences a central route of persuasion, but when elaboration is low, the recipient experiences a peripheral route (Petty and Cacioppo 1986). "Internet shoppers, especially those who perceive a high risk associated with online transactions, may proactively search for and carefully examine an e-tailer's privacy practices to alleviate their concerns about the privacy of their information" (Pan et al. 2006 p.332). On the other hand, when elaboration is low, individuals rely on simple decision criteria and cues such as design, endorsements, and attractiveness. Individuals use these cues either because they are not deeply involved in the issue, are not motivated enough to do so, or don't have sufficient knowledge about the subject matter. They do not devote the necessary cognitive energy or find themselves unable to expend the effort (Petty and Cacioppo 1986).

Research Model

We rely on ELM to conceptualize the moderating role of privacy concerns in determining the importance of privacy assurance mechanisms in increasing trust and enhancing the likelihood of information disclosure. The research model is shown in Figure 1 and discussed below.

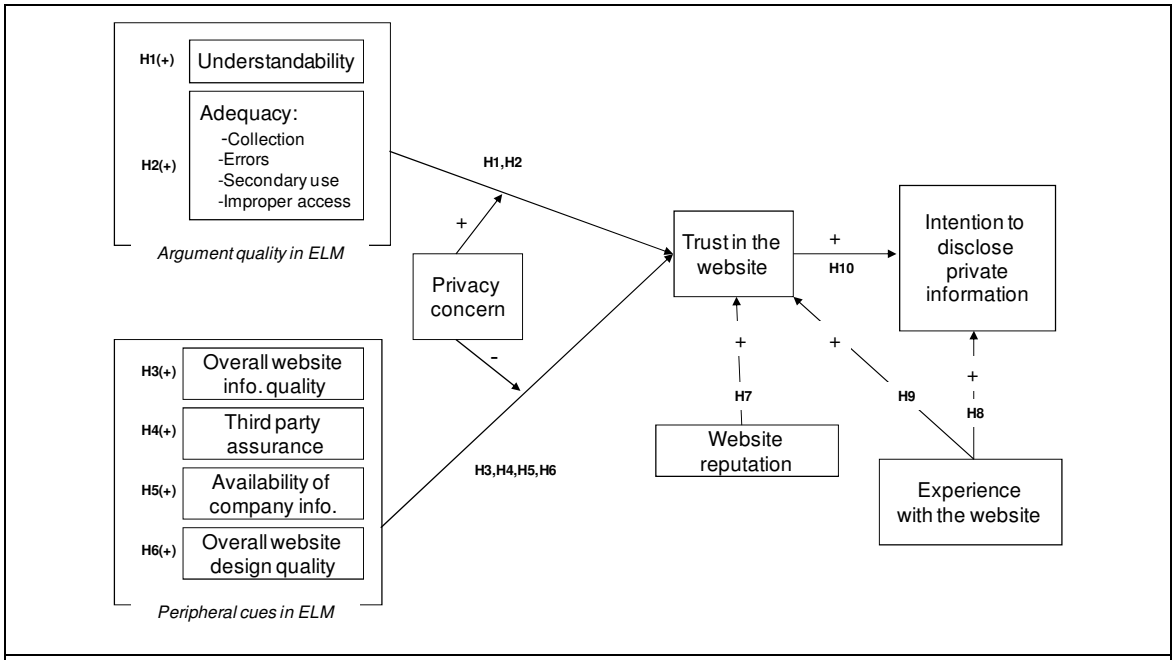

Figure 1. Research Model

Argument Quality (AQ)

Perceived Privacy Policy Understandability

The role of understandability of privacy-policy statements in increasing trust is an important and understudied issue. Pan and Zinkhan (2006) argue that a clearly stated privacy disclosure may be useful in alleviating privacy-related concerns. In turn, such a privacy policy may be expected to result in lower perceived risk (Miyazaki et al. 2000), and more trust in the store's fair information practices. Plain language should contribute to building trust in the vendor by reinforcing the notion that the web vendor is forthcoming and hence is reliable.

In various legal studies (e.g., Kimble 1994-1995) it has been argued that plain language improves comprehension, whereas traditional legal wording (legalese) does not communicate as well and may produce unnecessary confusion. Pan and Zinkhan (2006) argued that a straightforward privacy policy will result in more consumer trust in an online store than a long legalistic policy.

Even though it is known that readability of such statements might be associated with trust, studies have found that websites tend to post lengthy and incomprehensible privacy policy statements. Analyzing 40 online privacy policy statements, Westin (2004) reported that an average educational level of 14.1 years of schooling is needed to

understand the policies. A high percentage (49%) of the US adult population has no college education (March 2000 US Census data). Similarly, Milne et al. (2006) reported that during the time period of their study (2001–2003), the readability quality of privacy policy statements actually went down.

The research literature on notices and labels suggests that highly involved people read the food notices and labels more carefully than less concerned individuals (Szykman et al. 1997). Similarly, it could be argued that individuals with high privacy concern (PC) read the privacy policy statements more thoroughly before making an informed decision. The argument has support in ELM, which suggests that it is the highly involved who are more influenced via the central route, i.e. through the understandability of the privacy policy statement (a form of argument quality). In other words, PC should moderate the influence of understandability of privacy policy.

Hypothesis1. High privacy concern positively moderates the influence of understandability of privacy-policy statement on trust.

Perceived Adequacy of Privacy Policy Statement

Even though it is suggested that the mere presence of a privacy-policy statement builds trust, Earp et al. (2005), on the basis of their study of 50 websites and survey of over 1000 internet users, suggested that discrepancies exist between users' expectations and what privacy policies state. Other studies that examined the compliance of privacy-policy statements with the Federal Trade Commission's (FTC) fair information principles (FIP) concluded that there are many grave discrepancies. For instance, Adkinson et al. (2002) reported that only 60% notified visitors about the type of private information collected, fewer than half provided a choice about the use of information, and slightly more than half provided information about steps taken to provide security. Similarly, Peslak (2006) reported "limited compliance" with FIP[1] (notice, choice, access, and security).

A study of the Fortune E-50 found that only two of the top 50 e-companies fully complied with the four FTC's FIPs. Access and Security FIPs had the largest degrees of non-compliance (Ryker et al. 2002).

Table 1. Elements of Privacy Concerns and FTC Principles of Fair Information Practice

Smith et al. (1996)	FTC (2000)
Collection	**Notice:** Data collectors must disclose what personal information they collect from consumers.
Errors	**Access:** Consumers should be able to view and contest the accuracy and completeness of data collected about them.
Unauthorized secondary use (internal and external)	**Choice:** Consumers must be given options with respect to (1) whether and (2) how personal information collected from them may be used for purposes beyond those for which the information was provided.
Unauthorized access	**Security:** Data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

Absolute compliance with FIPs is important, but is a rather elusive target. Hence, this study focuses on the perceived adequacy of such statements, and argues that it should be important in determining trust intentions. This is somewhat supported by Meinert et al. (2006), who observed that willingness to provide information increases as the level of privacy guaranteed by the statements increases. Also Milne and Boza (1999) argued that privacy statements that are perceived to be informative and assure customers that disclosing their personal information does not involve risk, build trust in the website.

Independent of the FTC, Smith et al. (1996) developed and validated a scale to measure privacy concern. They argued that privacy concern is a second-order construct comprising concerns related to collection, unauthorized

[1] Based on the FTC (2000) Fair Information Practices in the Electronic Marketplace Report to Congress, Miyazaki and Krishnamurthy (2002 p. 35) noted that "common practice suggests that there are four fair information practice principles." These are notice, choice, access, and security. These are the privacy policy guidelines which corporations should adhere to as part of their fair information practices.

secondary use, errors, and unauthorized access. Table 1 juxtaposes the FTC's principles and Smith et al.'s (1996) constructs, showing that both documents support the same underlying definitions.

Based on this overlap, we define privacy-policy statement adequacy as a second-order construct, comprising the perception of Web users that the website (via its privacy-policy statement) is demonstrating adequate measures to handle their information privacy concerns related to collection, unauthorized secondary use, errors, and unauthorized access. Based on the ELM, individuals with high PC should be more influenced by the perceived adequacy (argument quality) of the privacy-policy statement.

Hypothesis2. High privacy concern positively moderates the influence of the adequacy of privacy-policy statement on trust.

Peripheral Cues

Perceived Website Information Quality. Nicolaou and McKnight (2006 p.335) demonstrated that users' "cognitive beliefs about the favorable or unfavorable characteristics of the currency, accuracy, completeness, relevance, and reliability" of the information during an exchange session can help build trusting beliefs. Although the information quality of a website is not a "main argument quality" for the privacy statement, research has shown that information quality plays a significant role in building trust and enhancing satisfaction (McKinney et al. 2002; Zahedi and Song 2008). Conversely, users who experience a website with poor information quality should have little reason to believe that the company behind the website could do any better with regard to other aspects of the service it provides, including its ability to safeguard their personal information. Therefore, in judging the privacy policies, information quality should be a major peripheral cue in building trust. This is a peripheral cue because, in contrast to H1 and H2 which dealt directly with the privacy-policy statement, this hypothesis deals with other non privacy-policy statement aspects of the website. Extending the logic of ELM implies that individuals with low PC, who tend to rely more on peripheral route, may rely on information quality, as a peripheral cue, in forming their trust to disclose their personal private information. Hence, we hypothesize that:

Hypothesis3. Low privacy concern positively moderates the influence of perceived information quality on trust.

Other Peripheral Cues. Trust seals like BBBOnline™ and TRUSTe™ increase consumer perceptions of a site's trustworthiness through transference. Research (Consumers International 2002) has found that website presentation quality (design quality) and availability of the contact details of the physical entity behind the website are associated with trust in the website. Web users rely on the design quality of the website to ascertain the degree of trust they can assign to the website. High design quality lowers risk beliefs associated with the website, and hence enhances the degree of trust. Users who lack the necessary motivation to delve deeper use such cues to form an impression about the trustworthiness of the site. This is in line with the ELM. The individuals with low PC are in a low elaboration state and rely on these peripheral cues for trust enhancement.

Hypothesis4. Low privacy concern positively moderates the influence of the perceived presence of third party endorsements on trust.

Hypothesis5. Low privacy concern positively moderates the influence of the perceived presence of company information on trust.

Hypothesis6. Low privacy concern positively moderates the influence of website design quality on trust.

Website Reputation

ELM considers source credibility as a peripheral cue, and one could argue that reputation is equivalent to source credibility. However, reputation, particularly in the online environment, is a far more important and universal variable than a peripheral cue. Reputation is the collective social knowledge about the trustworthiness of a website. It is often defined "in terms of the perception of a company's honesty with and concern towards its customers" (Metzger 2006 p. 157). Chiles and Mackin (1996) argued that reputation fosters the belief that a seller will act in the interest of the consumer. In the case of health infomediaries, Song and Zahedi (2007) reported a significant relationship between trust and reputation. Empirical research by Jarvenpaa et al. (1999, 2000), and Teo and Liu (2007) similarly suggest that the seller's reputation is an important characteristic that influences buyers' trust.

Hypothesis7. Reputation of a website is positively associated with trust in the website.

Past Positive Experience

Previous research supports the notion that prior positive experience is associated with trust in a website. Familiarity with a website affects consumers' trusting behavioral intentions (Gefen 2000; McKnight et al. 2002). In the context of health infomediaries, Song and Zahedi (2007) demonstrated that past positive experience leads to favorable trusting beliefs.

Hypothesis8. Prior positive experience with a website is positively associated with trust in the website.

Hypothesis9. Prior positive experience with a website is positively associated with increased intentions to disclose private information on the website.

Trust

Trust is the expectation that other individuals or companies with whom one interacts will not take undue advantage of a dependence upon them. It is the belief that the trusted party will behave in an appropriate manner and will fulfill all expected commitments (Luhmann 1979). Perceptions that the vendor is reliable encourage consumers to provide private information to the vendor (Dinev and Hart 2006; McKnight et al. 2002). Research shows that trust reduces perceived risk (Gefen et al. 2003), and hence provides the necessary comfort to the web user in disclosing one's information online. Hence,

Hypothesis10. Trust in a website is associated with intention to disclose private information.

Research Methodology

Operationalization of Variables

To increase construct validity we used items from existing scales wherever possible. The items' measurement was semantic differential (0-10). This was done to minimize common method bias. Table 2 reports the source of scales. The items used for argument quality and peripheral cues are shown in Table 3.

Table 2. Sources for Construct Items

Construct	Reference
Understandability of the Privacy Policy Statement	Self developed
Privacy Policy Adequacy (Collection, Errors, Secondary Use, Improper Access)	Adapted from Smith et al. (1996), FTC (2000)
Perceived overall website information quality	Nikolaou and McKnight (2006), McKinney et al. (2002)
Perceived Presence of third party assurances	Self-developed
Availability of company information	Self-developed
Perceived overall website design quality	Self-developed
Trust	Gefen et al. (2003)
Reputation	Zahedi and Song (2008)
Prior positive experience with the website	Song and Zahedi (2007)
Intention to disclose *(Finance / Personal /Health)*	Malhotra et al. (2004)
(Finance / Personal / Health) Information privacy concern	Malhotra et al. (2004)

Study Design

Based on a review of the literature (Rosenbaum 1973; Simmons 1968; Stone et al. 1989; Tolchinsky et al. 1981), Stone and Stone (1990) argued that perceived invasiveness differs across information types. Previous research has examined the level of privacy concern for different types of information, such as contact details, credit card number, social security number, and health information (Milne 1997; Phelps et al. 2000; Sheehan and Hoy 2000). However,

Table 3. Instrument (Argument Quality and Peripheral Cues)

Construct	Code	Items (All items were measured on a continuous 11-point semantic differential scale 0-10)
Understand-ability		With regards to the website privacy policy I just read, I believe that
	UND1	the level of difficulty associated with understanding of the privacy policy is (very high / very low)
	UND2	the number of confusing terms contained in the privacy policy is (very low / very high)
	UND3	the way the privacy policy was organized, it is (very hard to follow / very easy to follow)
	UND4	for my understanding, the length of the privacy policy is (way too much / just right)
	UND5	the privacy policy contained legal language that is (not clear at all / very clear)
Collection		Referring to the privacy policy which I just read; I believe that with regards to my private Information collected by the Website, the privacy policy's assurance that is
	COL1	collecting only the necessary information from me is (not adequate at all / very adequate)
	COL2	not collecting my private information for other purposes is (not adequate at all / very adequate)
	COL3	limiting information collection only to the minimum needed is (not adequate at all / very adequate)
Errors		Referring to the privacy policy which I just read, I believe that with regards to errors in my private information, the privacy policy's assurance
	ERR1	about the procedures to correct the error promptly is (not adequate at all / very adequate)
	ERR2	that I will be allowed to view and correct errors promptly is (not adequate at all / very adequate)
	ERR3	that my information will be checked for errors is (not adequate at all / very adequate)
	ERR4	that the accuracy of my private information will be maintained is (not adequate at all / very adequate)
Secondary Use		Referring to the privacy policy which I just visited, I believe that with regards to use of my private information for other purposes (such as promotional offers, sharing with other companies etc.), the privacy policy's assurance of
	SEC1	restricted use is (not adequate at all / very adequate)
	SEC	letting me authorize it before using it for other purposes is (not adequate at all / very adequate)
	SEC3	not-sharing it with others is (not adequate at all / very adequate)
	SEC4	allowing me to decide about the way my information is going to be used is (not adequate at all / very adequate)
Improper Access		Referring to the privacy policy which I just read, I believe that when it comes to unauthorized access to my private information,
	IMP1	the privacy policy's assurance of tight control is (not adequate at all / very adequate)
	IMP2	the privacy policy's assurance of protection is (not adequate at all / very adequate)
	IMP3	the measures stated to thwart unauthorized access are (not adequate at all / very adequate)
	IMP4	the level of efforts which the Website puts in to prevent theft is (very low / very high)
Information Quality		With reference to the website I just visited, I believe that the level of
	IQ1	currency (timeliness) of the information on this website is (not adequate at all / very adequate)
	IQ2	relevance of the information on this website to its customer to carry out his / her tasks is (not adequate at all / very adequate)
	IQ3	completeness of information on this website is (not adequate at all / very adequate)
	IQ4	reliability of information on this website is (not adequate at all / very adequate)
Third party endorsements		I believe that in the Website I just visited,
	END1	third party assurance seals (e.g., BBBOnline, TRUSTe) are (not present at all / present for sure)
	END2	third party assurances are (not displayed at all / displayed for sure)
	END3	assurances by trusted independent organizations are (not present for sure / present for sure)
Company Info.		I believe that in the Website I just visited,
	COMP1	contact email address is (not present at all / present for sure)
	COMP2	information about the physical location of the company is (not present at all / present for sure)
	COMP3	information about the contact phone number is (not present at all / present for sure)
Website Design Quality (Trusting Cues)		With reference to the Website I just visited, I believe that
	CUE1	the degree of the Website's design looking sloppy is (very high / very low)
	CUE2	the degree of the Website design looking professional is (very low / very high)
	CUE3	the Website's design quality is (very poor / very high)
	CUE4	the Website's layout looking business-like is (very low / very high)

no previous research examined how such sensitivity and related privacy concern moderate the influence of privacy assurance mechanisms on trust across various contexts. Extrapolating from Mayer et al. (1995), this should be the case because the level of vulnerability in providing private information on websites does vary by context. As the vulnerability increases, so should the reliance on trust in the decision to disclose such private information. This in turn allows for the development of a more realistic theory, which provides a more holistic view of privacy concern and trust relationships—a view that can help managers deal with such concerns in different ways. Furthermore, Whetten (1989), in discussing what constitutes theoretical contribution, lists four primary elements for a theory: what (constructs and concepts), how (relationships), why (underlying reasons), and who, where, and when (conditions and constraints). Addressing this concern, this paper focuses on not only "what", "how" and "why" but on the "where" (context) aspects as well. Hence, we tested the model across three different contexts using a controlled lab experiment with online access.

There were nine websites in total (Finance: www.chase.com, www.huntingtonbank, www.bendigobank.co.au; Health: www.webmd.com, www.everybody.co.nz, www.healthscout.com; E-commerce (travel): www.orbitz.com, www.shermantravels.com, www.bahamabeachclub.com). The websites were chosen so that they differed in terms of trust and reputation. Participants were students in a large Midwestern university. Participants were randomly assigned to view three websites (one finance website, one e-commerce website, and one health website). The participants were primed about the type of information involved in each context by asking about their sensitivities related to each type of information namely financial, personal and health. They were asked to browse through each website one by one and form a general opinion of the website. They were also required to read the privacy-policy statement of each website and form an opinion about its perceived understandability and its adequacy regarding the handling of their privacy concern. After viewing the website stimulus and reading its privacy-policy statement, each participant first answered a set of questions about the name and the nature of the website to ensure adequate surfing of the website. They then filled out the instrument online. This process was repeated for each of the three websites randomly assigned to the participant.

A total of 674 observations were collected. Factor scores for the privacy-concern construct (captured in the process of factor analysis) were used to categorize individuals into high PC (positive factor scores) or low PC (negative factor scores, inclusive of zero) groups. Table 4 reports sample sizes and group demographics.

Table 4. Demographics

	Finance				e-Commerce				Health			
	High PC Dataset		Low PC Dataset		High PC Dataset		Low PC Dataset		High PC Dataset		Low PC Dataset	
	Fem-ale	Male	Fem-ale	Male	Fema le	Male	Fem-ale	Male	Fem-ale	Male	Fem-ale	Male
N	218	148	181	127	173	148	226	127	215	101	184	174
Age Avg	20.21	20.31	21.21	21.17	20.67	21.33	20.65	20.00	20.70	21.18	20.63	20.28
Std Dev	2.33	3.20	4.31	5.75	3.98	5.65	2.90	2.73	3.90	5.87	2.99	2.93

Analysis and Results

Data Analysis

The observations for the three contexts were separated, and data for each context were divided into high and low PC. This led to six datasets, which were used for six model estimations (high-low finance, high-low e-commerce/personal, and high-low health). Data analysis was carried out in multiple steps. We followed the approach suggested by Song and Zahedi (2005) and McKinney et al. (2002) for data analysis. We first examined the discriminant and convergent validity of each of these six datasets separately. We also carried out six confirmatory factor analyses. The resulting factor loadings and fit indices provided support for the discriminant and convergent validity of the constructs. Factor loadings coefficients of all items were high (except for one item in the experience construct in the low-concern e-commerce context). The t-values were well above the 2.54 threshold (ranging from 4.98 to 73.93), supporting the statistical significance of factor loadings. We conducted the exploratory factor

analysis (EFA) of the second order construct in order to further examine the discriminant and convergent validity of the construct using six datasets separately. No cross-loadings above 0.4 were observed (except for one marginal case, where one item in one dataset (high PC in the health context) was observed with a cross loading of .402. We kept this item since it did not cross load in the other five estimations). All the items loaded together into the intended factor, supporting the discriminant validity of the proposed constructs. We examined the reliability of the measures. The Cronbach Alpha values were analyzed separately for each of the six datasets and were found to be greater than the suggested threshold of 0.70, except for two cases— "past positive experience with the website" for high and low PC in the e-commerce context, where the Cronbach alpha values were 0.69 and 0.68 respectively. We tested the datasets for the presence of common method variance, using the Harman's single factor test (Podsakoff et al. 2003). We found evidence of common method variance. In order to minimize the common method variance, we purified the datasets of three contexts by regressing each item with a common item and capturing residuals as the purified data (Podsakoff et al. 2003). We then used the residuals to conduct the analysis. The fit indices for the measurement and estimation models using the purified data are reported in Table 5.

Table 5. Fit Indices (using the Purified Data)

Fit Index	Measurement Model						Estimation Model					
	Finance		e-Commerce		Health		Finance		e-Commerce		Health	
	High PC	Low PC	High PC	Low PC	High PC	Low PC	High PC	Low PC	High PC	Low PC	High PC	Low PC
Normed chi-sq	1.446	1.285	1.446	1.550	1.418	1.495	1.463	1.284	1.452	1.554	1.420	1.504
CFI	0.949	0.963	0.956	0.953	0.958	0.958	0.947	0.963	0.955	0.952	0.958	0.957
TLI	0.945	0.960	0.952	0.949	0.955	0.954	0.943	0.960	0.952	0.948	0.954	0.953
RMSEA	0.035	0.030	0.037	0.039	0.036	0.037	0.036	0.030	0.038	0.040	0.036	0.037
SRMR	0.051	0.050	0.052	0.052	0.052	0.051	0.056	0.051	0.055	0.054	0.054	0.056

The fit indices are all within their respected thresholds, providing support for model fit. Next, the data were analyzed with a structural equations modeling approach using MPlus 4.1 (Muthén and Muthén 2007).

Results

Figure 2 shows the results for high PC and low PC in the finance context. Figure 3 shows the results in the e-commerce context, and Figure 4 shows the results in the health context. Table 6 reports summary results for all the three contexts. The results identify three types of PC moderation: structural, chi-square differences and coefficient differences. In the structural moderation, PC moderates the statistical significance of the path in that the path is significant for, say, low PC and not significant for high PC. This is a strong moderation effect. The second type of moderation is based on the chi-square test. Here we constrained each path one at a time to be equal in the high and low PC groups, and carried out a chi-square test of the constrained model with that of a regular non-constrained model. We did this chi-square moderation test for all those paths which were found to be significant for both high and low-level PC in each context. This too is a strong moderation effect. The third type of moderation is when a path coefficient, say for low PC, is statistically different from that for high PC based on a pairwise t-test—hence coefficient difference. When the t-test is not significant, then no moderation effect exists. When a path in both high and low PC is statistically not significant, the moderation effect cannot be tested.

In H1, we hypothesized that high PC positively moderates the impact of understandability of privacy-policy statement (as the ELM's argument quality) on trust in the website. This hypothesis was supported in the health context, showing that high-PC individuals rely on the understandability of the privacy-policy statement to form their trust in the website.

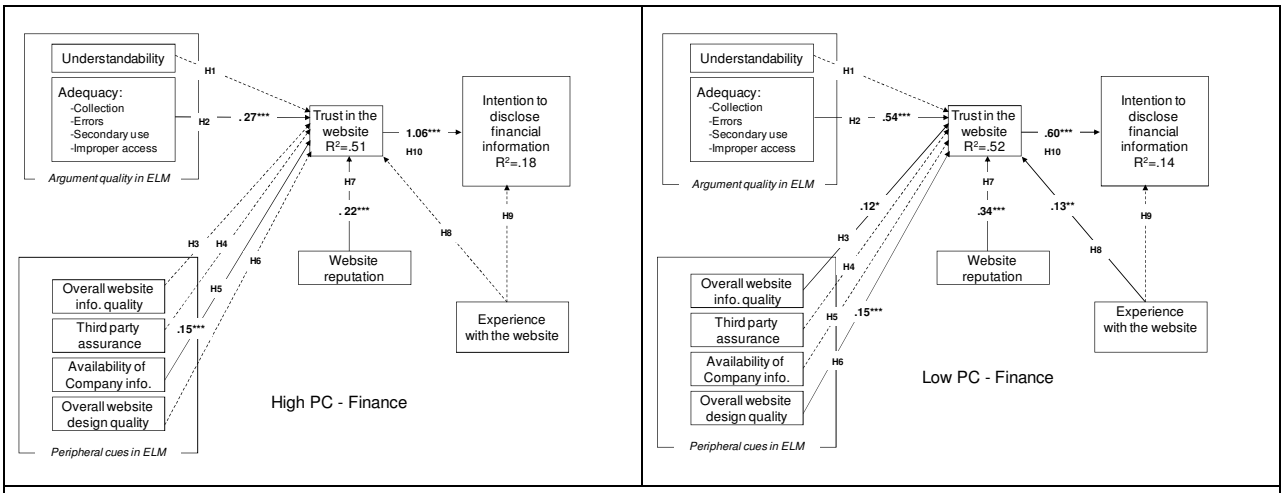

Figure 2. Model Estimations for High and Low PC in Finance

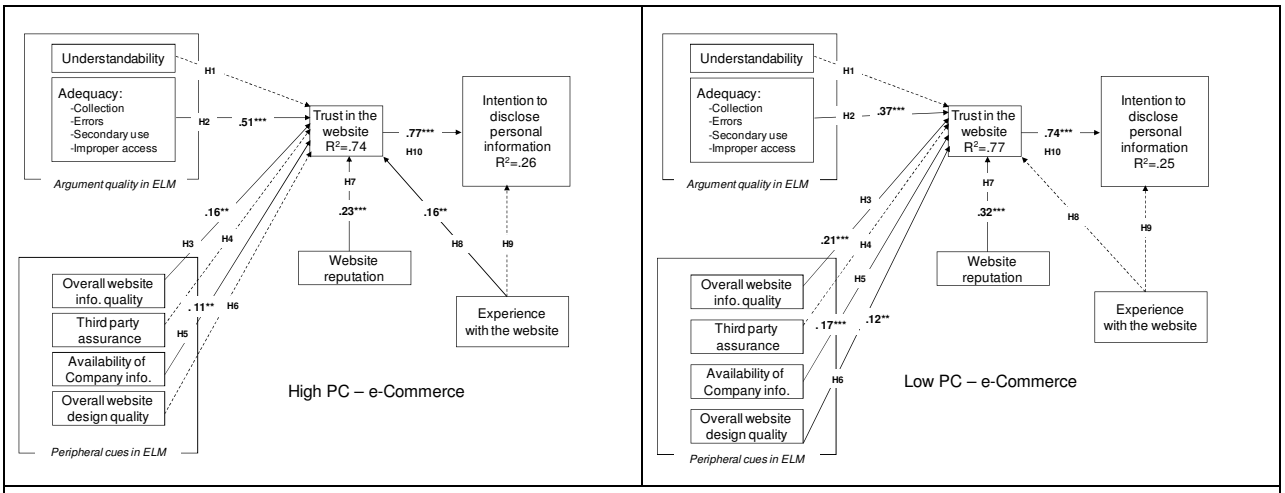

Figure 3. Model Estimations for High and Low PC in e-Commerce

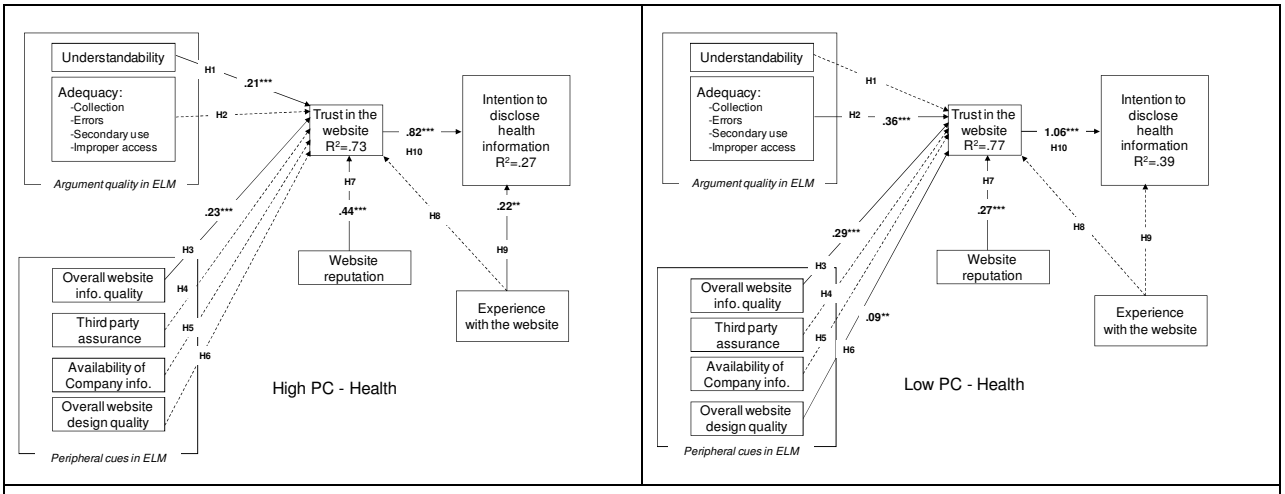

Figure 4. Model Estimations for High and Low PC in Health

Table 6. Result Summary			
	Finance	E-Commerce	Health
Privacy Policy Statement's Argument Quality→Trust (High PC vs. Low PC)			
H1-Understandability	ns	ns	**Supported**
H2-Adequacy	**Reverse Supported**	**Supported**	**Reverse Supported**
Peripheral Cues→Trust (High PC vs. Low PC)			
H3-Info. Quality	**Supported**	Both paths are significant but equal	**Supported**
H4-Endorsement	Ns	Ns	Ns
H5-Company Info.	**Reverse Supported**	**Supported**	ns
H6-Design Quality	**Supported**	**Supported**	**Supported**
Common Constructs			
H7-Reputation→Trust	**Supported**	**Supported**	**Supported**
H8-Experience→Trust	**Supported for low PC**	**Supported for high PC**	Ns
H9-Experience→Int. to disc.	Ns	Ns	**Supported for high PC**
H10-Trust→Int. to disc.	**Supported**	**Supported**	**Supported**

ns = both paths (for high and low PC) are insignificant, hence moderation could not be tested.

Furthermore, this moderation is structurally influential in that for low-PC individuals, understandability has no significant influence on trust. Hence, H1 provides some evidence for the ELM argument that in that high-PC individuals rely only on the central route (in this case understandability of privacy-policy statement).

H2 is supported only in the case of e-Commerce. Since health and finance are considered to be more sensitive contexts (Bansal et al. 2008, Malhotra et al. 2004), it could be possible that building trust in sensitive contexts requires something more than just adequacy of the privacy policy statement. H3 is mostly supported. The results show that information quality significantly influences trust in all contexts and PC levels except for high PC in finance, indicating a critical role of this construct in trust building. In support of H3, low PC positively moderated the impact of information quality on trust in the finance and health contexts. This moderation was structural in finance in that the path of information quality to trust was not significant in high PC, showing a strong moderating effect of PC in the finance context. In the e-commerce context, information quality significantly and equally influenced trust in both high and low PC.

In testing H4, we found that third party endorsements did not have any significant influence on trust in any of the three contexts, indicating that third party endorsement as a peripheral cue does not play any role in trust building in the contexts we considered.

In H5, we hypothesized that low PC moderates the influence of company information (as a peripheral cue for privacy-policy statement) on trust. In the context of e-commerce, H5 was supported in that low PC positively moderated the influence of company information on trust. The path coefficient of company information to trust was statistically significant for both high and low PC and the path coefficient of low PC was statistically greater than that in high PC. Therefore, in this context, low-PC individuals rely on company information to form their judgments about privacy practices of the website. However, in the context of finance, H5 was reverse supported. High PC positively moderated the influence of company information on trust, indicating that high-PC individuals rely on company information in the context of finance. Furthermore, company information was not significant in the health context either in low or high PC. The results show that the influence of company information on trust is context-dependent. Furthermore, the moderating effect of PC on the association between company information and trust is context-dependent as well.

The premise of H6 was that website design is a peripheral cue for the privacy practices of a website. Hence, we hypothesized that low PC positively moderates the influence of website quality on trust for disclosing private information online. This hypothesis was strongly supported for all three contexts, implying that website design quality is clearly a peripheral cue that only influences low PC individuals. This is the strongest supports since H6 is supported in all three contexts. Furthermore, the moderating effect of PC is structural in that design quality is significant only in low PC in all three contexts, showing a clear structural shift as the level of PC changes.

In H7, we hypothesized that reputation influences trust. The results support the hypothesis in all three contexts, indicating the universality of the influence of reputation on trust.

In H8 and H9, we hypothesized that past prior experience influences trust and intention to disclose private information online. Our results show that the influence of experience is context dependent. In the finance context, experience influences trust only in low PC. In the e-commerce context, experience influences trust only in high PC. In the health context, experience has no influence on trust. On the other hand, in H9, experience influences intention to disclose only in the health context and only for high-PC individuals. This indicates that experience influences decisions in different paths, depending on context and on the level of PC within each context.

Results for H10 reaffirm the findings reported in the literature that trust influences behavior intention, in this case, the intention to disclose private information online regardless of context or level of PC. However, as the post hoc analysis (shown in Table 8) indicates, PC moderates the influence of trust on intention to disclose in different contexts. The stringent chi square moderation tests show that PC moderates the relationship between trust and intention to disclose in health and finance contexts.

Table 7. Moderating Effect of PC on the Path Coefficients of Argument Quality and Peripheral Cues to Trust

Construct	High PC vs. Low PC Finance	High PC vs. Low PC E-Commerce	High PC vs. Low PC Health
Argument Quality→Trust			
Understandability	ns	ns	Only **high PC** path is sig.
Adequacy	**- *****	*******	Only **low PC** path is sig.
Peripheral Cues→Trust			
Info. Quality	Only **low PC** path is sig.	**- ***	**- *****
Company Info.	Only **high PC** path is sig.	**- *****	ns
Endorsement	ns	ns	ns
Design Quality	Only **low PC** path is sig.	Only **low PC** path is sig.	Only **low PC** path is sig.

ns = both paths (for high and low PC) are insignificant. (***)=p<0.001 for the difference between the two statistically significant paths. (*)= p<0.05.

To highlight the moderating influence of PC, the path coefficients of argument quality and peripheral cues to trust are compared for high-low PC in three contexts, as reported in Table 7. The results show a strong moderating effect of PC in all three contexts. Of 18 possible paths that PC could moderate in the three contexts, 12 paths were moderated by PC, of which 7 were structural moderations (where the path was significant only either for high or low PC group). 6 paths could not be tested since both high and low PC coefficients were insignificant. No chi-square differences were found. Hence, the results over all three contexts provide support for the main focus of the paper, indicating that privacy concern moderates the influence of argument quality and peripheral cues (as related to the quality of privacy-policy statement) on trust for disclosing private information online.

In order to investigate the moderating role of privacy concern more fully, we carried out a post hoc analysis to examine the moderating influence of PC on the remaining paths in the conceptualized model, including the path coefficients reputation → trust, experience → trust, reputation → intention to disclose, and trust → intention to disclose, as reported in Table 8. The results show that PC has a strong moderating effect for these relationships as well.

For the reputation → trust path, PC negatively moderates the influence of reputation on trust in the finance and e-commerce contexts, whereas PC positively moderates the influence of reputation in the health context. This

moderation is in the form of significant path differences. The chi-square moderation test shows that PC moderates the relationship between reputation and trust in health context.

In the post hoc examination of the paths from experience to trust and intention to disclose, the results indicate that the influence of past prior experience is highly context-dependent, and so is the moderating effect of PC. PC strongly moderates the influence of experience on trust in the context of finance and e-commerce, but has no moderating effect in the health context. On the other hand, PC moderates the influence of experience on intention to disclose information in the health context, but not in the other two contexts. Furthermore, PC moderates the influence of trust on intention to disclose in the three contexts.

An interesting outcome is that the direction of moderation is not uniform across the three contexts. For example, the direction of moderation is similar for finance and e-commerce in reputation→trust, and opposite in experience→ trust and in trust→intention to disclose. Of the three contexts, health has the most dissimilar moderation of the three contexts. This is an area that requires further investigation.

Table 8. Post Hoc Analysis

Construct	High PC vs. Low PC Finance	High PC vs. Low PC E-Commerce	High PC vs. Low PC Health
Reputation→Trust	**- *****	**- *****	***** (chi-square)**
Experience→Trust	Only **low PC** path is sig.	Only **high PC** path is sig.	ns
Experience→Int. to disc.	Ns	ns	**- *****
Trust→ Int. to disc.	***** (chi-square)**	**- *****	**- *** (chi-square)**

ns = both paths (for high and low PC) are insignificant. (***) $p<0.001$ for the difference between the two statistically significant paths.

Finally, in comparing the R^2 values of the dependents variables in the six estimated models, we found no major differences in R^2 for trust and intention to disclose between high vs. low PC estimated models in the finance and e-commerce contexts (Figures 2-6). However, in the health context R^2 value for intention to disclose was 0.27 for high PC and 0.39 for low PC, indicating the positive moderating effect of low PC on the ability of the model to explain the variation in intention to disclose in the health context. When we compared R^2 values across the three context, we found that the R^2 values of the two dependent variables (trust and intention to disclose) in finance were noticeably lower than those in e-commerce and health. In e-commerce and health, the R^2 value for trust was 0.74-0.78 as opposed to 0.50-0.52 in finance. Similarly, in e-commerce and health, the R^2 for intention to disclose was 0.26-0.39, whereas it was 0.15-0.18 in finance.

Discussion

The research question in this paper was whether individuals' privacy concern moderates the effect of the perceived quality of the privacy-policy statement and its peripheral cues on trust for disclosing private information online. The overall results of this study support a positive answer to this question and provide interesting insights and rich findings about the process of trust formation as related to the effect of the privacy-policy statement and its related cues in different contexts. Researchers and practitioners alike are interested in examining the generalizability of the theoretical proposals. It is argued that the "contextual" analysis prevents over-generalization, explains inconsistencies caused by context, and provides an appreciation of the interplay of person and situation (Johns 2001). Our results provide support for this perspective, and point to the context-dependency of relationships associated with privacy and trust.

The results indicate that high and low PC individuals may use different strategies for forming a trusting view regarding the privacy policy of a website in disclosing their private information online in different contexts. This confirms the observation by Petty and Cacioppo (1981), who noted that non-experts primarily focus on peripheral cues (design and reputation) but also use the central routes (argument quality) in shaping their attitudes.

The e-commerce context provides the most clear-cut support for the ELM's central route vs. peripheral route in dealing with the privacy policy of websites. Individuals with high PC rely primarily on the adequacy of the privacy-policy statement, and to a lesser degree on the peripheral cues of the website's company's information and information quality. On the other hand, individuals with low PC rely less on the adequacy of the privacy policy (the

central route) and more on peripheral cues of company information and website design. Information quality is equally important for high and low PC individuals in e-commerce. Furthermore, individuals with high PC rely on both website reputation and their own past prior experience in forming their trust. Individuals with low PC tend to rely on reputation (and not their own past prior experience) in their trust formation. In the e-commerce context, it seems that experience is a central route and reputation is a peripheral route for trust formation to disclose personal private information online. Furthermore, PC does not have any moderating effect on the relationship of trust and intention to disclose information in this context.

This picture changes when the context is finance. Individuals with high PC primarily rely on the adequacy of the privacy-policy statement and company information and to a lesser degree on website reputation to form their trust in disclosing their private financial information online. The role of trust in such a disclosure is quite high. Individuals with low PC rely not only on the adequacy of the statement but also on a number of peripheral cues, including information quality, web design quality, reputation and experience in forming their trust. Furthermore, in the finance context, high PC positively moderates the influence of trust on intention to disclose private financial information online, which indicates a higher sensitivity in this context.

While understandability of privacy-policy statement has no effect on trust in e-commerce and finance contexts, it plays a significant role in the health context. In this context, individuals with high PC rely on the understandability of the statement as well as information quality to form their trust. Reputation and experience play a significant role for them as well. Individuals with low PC use the adequacy of the statement as well as the peripheral cues—website information quality, design quality and reputation—in forming their trust. A surprising finding in this context is that PC has a negative moderating effect on the influence of trust on intention to disclose private health information online. It could be that individuals with high PC in the health context are the only group that uses prior experience directly in forming their decision to disclose their health information online.

While there are contextual differences in the strategies individuals use to deal with privacy issues in disclosing private information online, a number of common themes have also emerged. As the central route, either understandability or adequacy of privacy-policy statements has a significant role in trust formation to disclose private information in every context and in both high and low PC. Of the two constructs, adequacy of statement has a more prominent role. Furthermore, across all contexts and PC groups, we found no evidence in support of the influence of third-party assurance as a peripheral cue for the building trust in a website. On the other hand, we found strong evidence in support of website information quality and website design quality as peripheral cues in lieu of privacy policy. Furthermore, reputation alone or in combination with company information is a strong peripheral cue, which in some cases could be a viable complement for the statement quality.

These findings have a number of theoretical and practical implications. On the theoretical ground, we have extended the application of the elaboration likelihood method to privacy concern and trust in disclosing private information online. This study is the first to examine in some detail the moderating influence of privacy concern on the way a privacy-policy statement (as a central route) and peripheral cues (as the peripheral route) promote trust and increase individuals' willingness to disclose their private information online. Furthermore, our work extends ELM and theories related to trust and privacy in providing strong evidence that context matters, and trust relationships should be examined in different contexts. A cross-context analysis of trust and privacy issues could distinguish generalizability versus context-specificity of relationships, both of which provide a deeper understanding of online user behaviors. Our findings add to the trust literature by highlighting the influence of level of privacy concern (as "who") and context (as "where") (Whetten 1989). The paper also adds to ELM by demonstrating the moderating role of context over and above the moderating role of degree of involvement (privacy concern).

Furthermore, we found that the adequacy of a privacy-policy statement is such a strong part of the message that almost all individuals in different contexts pay close attention to it. This could extend ELM's dichotomy of central vs. peripheral route to include a third route—a "universal" route. The universal route may consist of critical parts of the message that individuals, regardless of their level of involvement, invest cognitive energy to process. Identifying the features that are processed through the universal route could be an important undertaking in behavioral studies in the online environment in general and for trust studies in particular.

Our findings also have practical implications. They indicate that privacy issues may not be addressed just by posting a privacy-policy statement. The overall message from this study for managers is that individuals use a number of cues and variables to form their opinions about how an online company may deal with their private information.

Dealing with privacy concerns requires a holistic plan and continuous vigilance. The managers should recognize that privacy issues are context-dependent. Furthermore, individuals with different degrees of privacy concern need a variety of mechanisms for privacy assurance. These mechanisms include the understandability and adequacy of the privacy-policy statement. Of the two, adequacy is more critical. The statement should adequately address issues related to the way private data is collected, the way errors are handled, and assurances about secondary use, unauthorized access, and use of private data. Although necessary, a clear and adequate privacy-policy statement will not be sufficient to alleviate individuals' privacy concerns. Information quality and website-design quality are surrogates for privacy practices. Furthermore, managers should be aware of the importance of company information and reputation in easing their customers' privacy concern. In other words, a privacy-policy statement is just one piece of the three-piece puzzle in dealing with privacy concerns. The way a company is presented and viewed by the social community is the second piece. The third piece is the quality of the website content and design. Individuals with different levels of privacy concern and in different contexts use a combination of these three pieces to form a trusting attitude in providing their private information. Companies need to find ways to understand the extent of their customers' privacy concern and provide them with a possibly personalized mix in order to deal with their privacy issues and ultimately establish a closer tie with their customers.

Limitations

We start this section with the limitations of this study. The study has limited generalizability since the sample was based on college students living in the Midwest. All items were self-reported, including the intention to disclose. This study should be repeated with samples drawn from other population types, including older or less educated individuals.

Conclusions and Future Directions

Previous research (Meinert et al. 2006; Milne and Boza 1999; Milne and Culnan 2002, 2004; Pan et al. 2006) showed that privacy policy statements and privacy assurance cues help consumers make a more accurate assessment of the risks of disclosing private information to websites. Previous research, however, has not adequately dealt with the dynamics of the influence process, the moderating impact of privacy concern, and the role of context. This study addresses this gap by elaborating on two alternating means of influence—a central route consisting of the understandability and adequacy of the privacy-policy statement and a peripheral route consisting of a number of peripheral cues for the privacy practices. In this study, we applied the ELM, and our results led to its extension by introducing the possible existence of a "universal" route. The results of this study also show distinct behavioral differences among individuals with high as opposed to those with low privacy concern in forming their trust to disclose private information across different contexts. As such, this study adds to the trust literature by highlighting the influence of privacy concern as a significant personal "who" factor and context as "where" factor.

At the managerial level, this study highlighted the importance of a holistic strategy in dealing with customers' privacy concern. Privacy-policy statements only work within a broader structure that involves website information quality and overall design. In other words, the most comprehensive and clear privacy-policy statement will be of little consequence if the website lacks assurances generated by the quality of website information and design. An unprofessional look or inaccurate information could easily offset the positive influence of the most elaborate privacy-policy statement. Added to this mix are company information on the website and its reputation within the social community of users. The recognition of the strong moderating influence of individuals' privacy concerns within different context is also needed in order to provide a tailored mix of cues that reinforce the impact of privacy-policy statements.

In a global society in which reliance on the Web for the delivery of services is rapidly increasing, issues related to privacy require a closer examination in order to inspire trust for disclosing private information needed to receive these services, such as medical advice, financial assistance or personal services. Our work shows that general and uniform publication of privacy statements may not be adequate for dealing with the privacy concern of all individuals in various contexts. Rather, it points to the direction of personalized privacy assurance in different contexts. This is a line of study that requires further investigation and deeper elaborations in the future studies.

References

Adkinson, W., Eisenrach, J., and Lenard, T. "Privacy Online: A Report of the Information Practices and Policies of Commercial Web Sites," Retrieved from http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf [last accessed July 15, 2007], 2002.

Bansal, G., Zahedi, F.M., and Gefen, D. "Context and Personality Do Matter: Trust and Privacy Concern in Disclosing Sensitive Information Online," Working Paper, *University of Wisconsin – Milwaukee*, 2008.

Benassi, P. "TRUSTe: An Online Privacy Seal Program", *Communications of the ACM* (42:2), 1999, pp. 56-59.

Chiles, T.H., and McMackin, J.F. "Integrating Variable Risk Preferences, Trust, and Transaction Cost Economics," *Academy of Management Review* (21:1), 1996, pp. 73-99.

Consumers International, *Credibility on the Web* (ISBN: 1-902391-39-X), 2002

Dinev, T., and Hart, P. "An Extended Privacy Calculus Model for E-Commerce Transaction," *Information Systems Research* (17:1), 2006, pp. 61-80.

Earp, J.B., Anton, A.I., Aiman-Smith, L, and Stufflebeam, W. H. "Examining Internet Privacy Policies within the Context of User Privacy Values," *IEEE Transactions of Engineering Management* (52:2), 2005, pp. 227-237.

Earp, J.B., and Baumer, D. "Innovative Web Use to Learn about User Behavior and Online Privacy, *Communications of ACM* (46:4), 2003, pp. 81-83.

Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to the Congress,* Retrieved from http://www.ftc.gov/reports/privacy2000/privacy2000.pdf [last accessed April 27, 2008]

Gefen, D. "E-commerce: The Role of Familiarity and Trust," *Omega* (28:5), 2000, pp. 725-737.

Gefen, D., Karahanna, E., and Straub, D.W. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), 2003, pp. 51-90.

Hui, K-L., Teo, H.H., and Lee, S.T. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly* (31:1), 2007, pp. 19-33.

Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. "Consumer Trust in an Internet Storey," *Information Technology Management* (1), 2000, pp. 45-71.

Jarvenpaa, S.,L., Tractinsky, N., Saarinen, L., and Vitale, M. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer Mediated Communications* (5:2), 1999, pp. 44-71.

Johns, G. "In the Praise of Context," *Journal of Organizational Behavior* (22), 2001, pp. 31-42.

Johns, G. "The Essential Impact of Context on Organizational Behavior," *Academy of Management Review* (31:2), 2006, pp. 386-408.

Kimble, J. "Answering the Critics of Plain Language," *Scribes Journal of Legal Writing* (5), 1994-1995, pp. 51. [available at http://www.plainlanguagenetwork.org/kimble/Anwering2.pdf last accessed April 27, 2008]

Liu, C., and Arnett, K. "An Examination of Privacy Policies in Fortune 500 Web Sites," *Mid-American Journal of Business* (17:1), 2002, pp. 13-22.

Luhmann, N. *Trust and Power*, John Wiley and Sons, London, U.K, 1979.

Malhotra, N.K., Kim, S.S., and Agarwal, J. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), 2004, pp. 336-355.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. "An Integration Model of Organizational Trust," *The Academy of Management Review* (20:3), 1995, pp. 709-735.

McKinney, V., Yoon, K., and Zahedi, F.M. "The Measurement of Web-Customer Satisfaction: An Expectation and Disconfirmation Approach," *Information Systems Research (13:3),* 2002, pp. 296-315.

McKnight, D.H., Choudhury, V., and Kacmar, C. "Developing and Validating Trust Measures for E-Commerce: An Integrative Typology," *Information Systems Research* (13:3), 2002, pp. 334-359.

Meinert, D.B., Peterson, D.K., Criswell, J.R., and Crossland, M.D. "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," *Journal of Electronic Commerce in Organizations* (4:1), 2006, pp. 1-17.

Metzger, M.J. "Effects of Site, Vendor, and Consumer Characteristics on Web Site Trust and Disclosure," *Communication Research* (33:3), 2006, pp. 155-179.

Milne, G.R. "Consumer Participation in Mailing Lists: A Field Experiment," *Journal of Public Policy & Marketing* (16:2), 1997, pp. 298-309.

Milne, G.R., and Boza, M. "Trust and Concern in Consumers' Perception of Marketing Information Management Practices," *Journal of Interactive Marketing* (13:1), 1999, pp. 5-24.

Milne, G.R., and Culnan, M.J. "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys," *The Information Society* (18:5), 2002, pp. 345-360.

Milne, G.R., and Culnan, M.J. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing* (18:3), 2004, pp. 15-29.

Milne, G.R., Culnan, M.J., and Greene, H. "A Longitudinal Assessment of Online Privacy Notice Readability," *American Marketing Association* (25:2), 2006, pp. 238-249.

Miyazaki, A.D., and Fernandez, A. "Internet Privacy and Security: An Examination of Online Retailer Disclosures," *Journal of Public Policy & Marketing* (19:1), 2000, pp. 54-61.

Miyazaki, A.D., and Krishnamurthy, S. "Internet Seals of Approval: Effects of Online Privacy Policies and Consumer Perceptions," *The Journal of Consumer Affairs* (36:1), 2002, pp. 28-49.

Muthén, L.K., and Muthén, B.O. *Mplus Statistical Analysis with Latent Variables* (Version 4.1), Muthén & Muthén, Los Angeles, CA, 2007.

Nicolaou, A., and McKnight, D.H. "Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use," *Information Systems Research* (17:4), 2006, pp. 332-351.

Pan, Y., and Zinkhan, G.M. "Exploring the Impact of Online Privacy Disclosure on Consumer Trust," *Journal of Retailing* (82:4), 2006, pp. 331.

Peslak, A.R "Internet Privacy Policies of the Largest International Companies," *Journal of Electronic Commerce in Organization* (4:3), 2006, pp. 46-62.

Petty, R.E., and Cacioppo, J.T. *Communication and Persuasion: Central and Peripheral Routes to Attitude Change,* Springer-Verlag, New York, 1986.

Petty, R.E., Cacioppo, J.T., and Goldman, R. "Personal Involvement as a Determinant of Argument-Based Persuasion," *Journal of Personality and Social Psychology* (41:5), 1981, pp. 847-855.

Phelps, J., Nowak, G., and Ferrell, E. "Privacy Concerns and Consumer Willingness to provide Personal Information," *Journal of Public Policy & Marketing* (19:1), 2000, pp. 27-41.

Podsakoff, S., MacKenzie, B., Lee, J.Y., and Podsakoff, N.P. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), 2003, pp. 879-903.

Pollach, I. "Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions," *Journal of Organizational and End User Computing* (18:1), 2006, pp. 23-49.

Rosenbaum, B.L. "Attitude toward Invasion of Privacy in the Personnel Selection Process and Job Applicant Demographic and Personality Correlates," *Journal of Applied Psychology* (58), 1973, pp. 333-338.

Ryker, R., Lafleur, E., McManis, B., and Cox, K.C. "Online Privacy Policies: An Assessment of the Fortune E-50," *The Journal of Computer Information Systems* (42:4), 2002, pp. 15-20.

Sheehan, K.B., and Hoy, M.G. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), 2000, pp. 62-73.

Simmons, D.D. "Invasion of Privacy and Judged Benefit of Personality Test Inquiry," *The Journal of General Psychology* (79), 1968, pp. 177-181.

Smith, J.H., Milberg, S.J., and Burke, S.J. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), 1996, pp .167-196.

Song, J., and Zahedi, F.M. "Trust in Health Infomediaries," *Decision Support Systems* (43), 2007, pp. 390-407.

Song, J., and Zahedi, F.M. "A Theoretical Approach to Web Design in E-Commerce: A Belief Reinforcement Model," *Management Science* (51:8), 2005, pp. 1219-1235.

Stone, E.F., and Stone, D.L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8), 1990, pp. 349-411.

Stone, E.F., Stone, D.L., and Hyatt, D. "Personnel Selection Procedures and Invasion of Privacy," in R. Guion (chair), *Privacy in Organizations: Personnel Selection, Physical Environment, and Legal Issues*, Symposium conducted at the annual conference of the Society for Industrial and Organizational Psychology, Boston, MA, 1989.

Szykman, L.R., Bloom, P.N., and Levy, A.S. "A Proposed Model of the Use of Package Claims and Nutrition Labels," *Journal of Public Policy and Marketing* (16:2), 1997, pp. 228-241.

Teo, T.S.H., and Liu, J. "Consumer Trust in e-Commerce in the United States, Singapore and China," *Omega* (35:1), 2007, pp. 22-38.

Tolchinsky, P.D., McCuddy, M., Adams, J., Ganster, D.C., Woodman, R., and Romkin, H.L. "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology* (66), 1981, pp. 308-313.

Westin, A.F. "How to Craft Effective Online Privacy Policies," *Privacy and American Business* (11), 2004, pp. 6, 1-2.

Whetten, D.A. "What Constitutes a Theoretical Contribution?" *Academy of Management Review* (14:4), 1989, pp. 490-495.

Zahedi, M.F., and Song, J. "Dynamics of Trust Revision: Using Health Infomediaries," *Journal of MIS* (24:4), 2008, pp. 225-248.